ECKERT SEAMANS ATTORNEYS AT LAW

March 22 2020

Data Security & Privacy Alert

# COVID-19 and Working Remotely: Data Security & Privacy Challenges

As companies are forced to hurriedly transition their workforce to remote status, safe practices for the collection, handling, and disposal of personal information and other sensitive data can easily be overlooked in the chaos.

Here are some of the steps companies can take to minimize information security and privacy risks:

- **Corporate data privacy and security principles.** These principles should already be a part of the culture and policy of the workplace, and should not change when employees suddenly find themselves working in an offsite environment. Companies must stress to remote employees that safe information storage and handling policies and practices are still in place, and are more important than ever to observe.
- **Others present in the home environment.** If an employee working remotely has access to personal information or other sensitive company data, the employee needs to be aware of the close presence of other people in the household who are not authorized to see what is on the employee's screen or in an open folder.
- **Close and lock devices.** For the reasons stated above, devices used at home for company business should be closed and locked when not in use.
- **Downloads to hard drives and flash drives.** Workplace networks and database storage systems may not be easily accessible to offsite employees, which may increase downloading of sensitive data to hard drives and flash drives. These data storage options tend to be more easily lost or stolen and may not be equipped with malware protection or encryption capability. Remind your remote employees to exercise increased care concerning the use of portable and home media for storage of sensitive information, and issue appropriate policies and procedures.
- **Are personal devices equipped with adequate security tools?** If the remote employee is using a personal device to handle work data or access work systems, how secure is that device? Is it equipped with the necessary safeguards to comply with company security standards? Companies should either: (1) ensure that employee personal devices have adequate security protections; or, (2) mandate that only employer-issued devices may be used for working with sensitive information.
- **Don't forget about paper.** If the remote employee printed something and brought it home, or prints to a home printer, they need to:
    - Secure the paper from access by unauthorized individuals (don't leave it laying around).
    - Observe the company document retention and safe destruction practices, which are in effect even when employees are working offsite.
- **Stress vigilance against COVID-19-related phishing and social engineering scams.** Sadly, cyber criminals wasted little time in capitalizing upon the confusion and fear surrounding the COVID-19 health crisis. For

example, bad actors are sending emails claiming to be from legitimate organizations with information about the coronavirus. These phishing email messages ask you to open an attachment to see the latest statistics or instructions from health or government agencies. However, clicking on the attachment or an embedded link may result in the downloading of malicious software.

- **Your IT professionals might not be focused on data security at the moment.** Taking the company to a remote operating platform on an urgent basis has probably given your IT department an imposing set of tasks to accomplish. Caution your employees that the IT team might be slower to respond to inquiries than normal, and to use common sense and err on the side of caution when in doubt about an action that could have data security risk implications before IT has been fully consulted.

During the COVID-19 health crisis, while individuals are being urged to take measures to protect the health of themselves and others, companies should remind and encourage their remote workforce to maintain good "information hygiene" practices, too.

ECKERT SEAMANS ATTORNEYS AT LAW